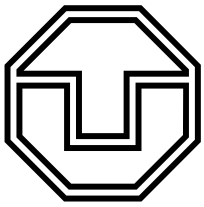

TECHNISCHE UNIVERSITÄT DRESDEN

Department of Mathematics
Bachelor's Thesis (B.Sc.)

Complete Arcs in Projective Spaces, the MDS Main Conjecture and Related Problems

Author:
Jakob Schneider
(* January 26, 1994, in Peine, Germany)

Supervisor:
Prof. Dr. Ulrich Brehm
(Institute of Geometry)

August 8, 2014
(date of submission)

To my grandma.
My thoughts and prayers are with you.

Statutory Declaration

I declare on oath that I completed this work on my own and that information which has been directly or indirectly taken from other sources has been noted as such. Neither this, nor a similar work, has been published or presented to an examination committee.

Dresden, August 8, 2014 Jakob Schneider

Erklärung

Hiermit erkläre ich, dass ich die am 8. August eingereichte Bachelorarbeit zum Thema *Complete Arcs in Projective Spaces, the MDS Main Conjecture and Related Problems* unter Betreuung von Prof. Dr. Ulrich Brehm selbstständig erarbeitet, verfasst und Zitate kenntlich gemacht habe. Andere als die angegebenen Hilfsmittel wurden von mir nicht benutzt.

Dresden, 8. August, 2014 Jakob Schneider

1 The proof of the MDS main conjecture for $n \leq 2p-2$

In the following we aim to present the results of the two papers [?] and [?] simplifying some aspects of the proofs.

1.1 Segre's lemma of tangents

Any attempt to answer the MDS main conjecture uses a lemma which was first stated by B. Segre and can be considered as a key result. To state it we need the following

[tangent polynomials] Let $\mathcal{A}$ be an arc in $\mathbb{F}_q^n$. Then for any $(n-2)$-set $X \subseteq \mathcal{A}$ define the tangent polynomial T_X as the product

$$T_X \coloneqq \prod_{\substack{H \in \operatorname{Sub} \mathbb{F}_q^n \\ \operatorname{codim} H = 1 \\ H \cap \mathcal{A} = X}} l_H$$

where l_H are linear forms such that $\ker l_H = H$. This defines (up to scalar factor from ${\mathbb{F}_q}^\times$) a homogeneous polynomial in n variables which is of degree $q+1-(\mathcal{A}-(n-2)) = q-1+n-|\mathcal{A}| =: t$ (by counting the corresponding hyperplanes).

The main idea of this section is to present a way to choose the tangent polynomials canonically with respect to a given order on the elements of the arc. This will simplify the calculation in the proofs of various lemmas a lot.

From $t \geq 0$ one gets the weak bound $|\mathcal{A}| \leq q+n-1$ which we already derived in sec-gen-hyperplane-arr.

Now we are able to state the lemma.

[Segre's lemma of tangents, original version] Let $n \geq 3$ and $\mathcal{A}$ be a representation of an arc in $\mathrm{P}\mathbb{F}_q^n$. Then for pairwise distinct $x_i \in \mathcal{A}$ $(i = 0, 1, 2)$ and $X \subseteq \mathcal{A} \setminus \{x_0, x_1, x_2\}$, $|X| = n-3$ we have

$$\frac{T_{X\cup\{x_0\}}(x_1) T_{X\cup\{x_1\}}(x_2) T_{X\cup\{x_2\}}(x_0)}{T_{X\cup\{x_1\}}(x_0) T_{X\cup\{x_2\}}(x_1) T_{X\cup\{x_0\}}(x_2)} = (-1)^{t+1}.$$

The expression in the lemma is well-defined since the scalar factors in T_Y vanish in the fraction.

Denote by x_i^* the linear form corresponding to x_i in the dual basis of $X' \coloneqq X \cup \{x_0, x_1, x_2\}$. For $i \in \{0,1,2\}$ let $\mathcal{H}_i$ be the set of hyperplanes H containing $\langle X, x_i \rangle$ but not x_j for $j \neq i$. For each hyperplane $H \in \mathcal{H}_i$ there are two possibilities:

There is an $a \in \mathcal{A} \setminus X'$ with $a \in H$. In this case define the linear form

$$l_H \coloneqq \det(\bullet, x_i, X, a)$$

Otherwise, l_H is already defined via the tangent polynomials. Now, one may define the polynomial $P_i \coloneqq \prod_{H \in \mathcal{H}_i} l_H$ (of degree $q-1$) and one computes that

$$P_i(x_j) = T_{X\cup\{x_i\}}(x_j) \prod_{a \in \mathcal{A}\setminus X'} \det(x_j, x_i, X, a).$$

When $\{0,1,2\} \setminus \{i\} = \{j,k\}$ it is clear that $P_i(x_j)/P_i(x_k) = -1$ which can be deduced from the fact that the product of all units of a finite field is -1 and the observation that all hyperplanes in $\mathcal{H}_i$ are given by $\ker(x_j^* + \lambda x_k^*)$ where $\lambda \in {\mathbb{F}_q}^\times$. Thus we have

$$\frac{P_1(x_1)P_2(x_2)P_3(x_0)}{P_2(x_0)P_3(x_1)P_1(x_2)} = \frac{T_{X\cup\{x_0\}}(x_1)T_{X\cup\{x_1\}}(x_2)T_{X\cup\{x_2\}}(x_0)}{T_{X\cup\{x_1\}}(x_0)T_{X\cup\{x_2\}}(x_1)T_{X\cup\{x_0\}}(x_2)} \tag{1}$$

$$\times \prod_{\substack{i,j\in\{0,1,2\}\\ i<j}} \prod_{a\in\mathcal{A}\setminus X'} \frac{\det(x_i,x_j,X,a)}{\det(x_j,x_i,X,a)} \tag{2}$$

$$= (-1)^3 = -1. \tag{3}$$

Since $\mathcal{A} \setminus X'$ has $|\mathcal{A}| - n = q - 1 - t$ elements, the last two products evaluate to $(-1)^{3(q-1-t)} = (-1)^t$. This finishes the proof.

For convenience we now state a 'simplified version' of SEGRE's lemma which is the only version we shall use in the following.

At first it becomes necessary to recall the meaning of the following notation from the preliminaries.

[sequence notation] By $(A_0, \ldots, A_{m-1})$ we mean the sequence as explained in not-conv where A_i is a subset of some ordered set A.

[Simplification of SEGRE's lemma] Let $\mathcal{A}$ be a representation of an arc in $\mathrm{P}\mathbb{F}_q^n$ ($n \geq 3$) and $\leq$ some linear order on $\mathcal{A}$. Then we can define the tangent polynomials T_Y ($Y \subseteq \mathcal{A}$, $|Y| = n-2$) such that for all x_0, x_1, X we have

$$\frac{T_{X\cup\{x_1\}}(x_0)}{T_{X\cup\{x_0\}}(x_1)} = \left(\frac{\operatorname{sgn}(X \cup \{x_1\}, x_0)}{\operatorname{sgn}(X \cup \{x_0\}, x_1)}\right)^{t+1}$$

where $X \subseteq \mathcal{A}$ has $n-3$ elements and $x_0, x_1 \in \mathcal{A} \setminus X$ are distinct.

We define the directed graph $G = (V, E)$ by $V := \binom{\mathcal{A}}{n-2}$ and $E := \{(u,v) \in V^2 : |u \setminus v| = 1\}$. Moreover, we define a labeling $\lambda : E \to {\mathbb{F}_q}^\times$. For $(u,v) \in E$ let $u_v \in u \setminus v$ and $v_u \in v \setminus u$ be the elements of the singletons. Then define

$$\lambda(u,v) := \frac{T_u(v_u)}{T_v(u_v)}.$$

For the two types of triangles in G we have two different relations holding. A triangle of the first type consists of vertices $u, v, w \in V$ such that $|u \cup v \cup w| = n-1$. Here it clearly holds that

$$\lambda(u,v)\lambda(v,w)\lambda(w,u) = \frac{T_u(v_u)T_v(w_v)T_w(u_w)}{T_v(u_v)T_w(v_w)T_u(w_u)} = 1$$

which is a trivial equation since $v_u = w_u$, $u_v = w_v$, $u_w = v_w$. For a triangle of the second type consisting of vertices $u, v, w \in V$ such that $|u \cup v \cup w| = n$ we obtain

$$\lambda(u,v)\lambda(v,w)\lambda(w,u) = (-1)^{t+1}$$

by segre-tangent-lemma-orig where $X \coloneqq u \cap v \cap w$ and $x_0 \coloneqq u_v = u_w$, $x_1 \coloneqq v_u = v_w$, $x_2 \coloneqq w_u = w_v$. It is thus clear, that λ is uniquely defined by any restriction $\lambda|_{E_T}$ where $T = (V, E_T)$ is a (directed) rooted spanning tree of G with root $r \in V$ (by the above relations in triangles of G and as G is obviously strongly connected). Moreover, when replacing T_u by $T'_u \coloneqq \mu T_u$ one just modifies λ to λ' where

$$\lambda'(v,w) = \begin{cases} \lambda(v,w) & : \text{u}\notin \{v,w\} \\ \mu\lambda(v,w) & : \text{v=u} \\ \mu^{-1}\lambda(v,w) & : \text{w=u} \end{cases} .$$

This idea can be used to modify the tangent polynomials step by step to achieve any values of λ among E_T. Define the sets $V_l \coloneqq \{v \in V : d_T(r,v) = l\}$ ($l \in \mathbb{N}$, here $d_T(\bullet_1, \bullet_2)$ means the metric of the shortest path on T). Since G is finite there is some $L \in \mathbb{N}$ such that $\{V_l : l = 0, \ldots, L\}$ is a partition of V. Moreover, one notes that the sets $E_l \coloneqq \{(u,v) \in E_T : u \in V_{l-1}, v \in V_l\}$ for $l = 1, \ldots, L$ form a partition of E_T. Thus one can modify the labeling λ at first on E_1 then on E_2 etc. As there is no edge in T between the sets V_m and V_n where $|n-m| \geq 2$ this procedure works and one does not destroy former changes on some E_i. This shows that λ can be changed to any labeling satisfying the two triangle conditions. Lastly, we check that these are satisfied for the labeling $\overline{\lambda}$ given in the lemma, where for $(u,v) \in E$

$$\overline{\lambda}(u,v) \coloneqq \left(\frac{\operatorname{sgn}(u,v_u)}{\operatorname{sgn}(v,u_v)}\right)^{t+1} .$$

For a triangle uvw of the first type ($|u \cup v \cup w| = n-1$) we obtain $v_u = w_u$, $u_v = w_v$, $u_w = v_w$ and thus one gets

$$\overline{\lambda}(u,v)\overline{\lambda}(v,w)\overline{\lambda}(w,u) = \left(\frac{\operatorname{sgn}(u,v_u)}{\operatorname{sgn}(v,u_v)}\frac{\operatorname{sgn}(v,w_v)}{\operatorname{sgn}(w,v_w)}\frac{\operatorname{sgn}(w,u_w)}{\operatorname{sgn}(u,w_u)}\right)^{t+1} = 1$$

Similarly, for a triangle uvw of the second type ($|u \cup v \cup w| = n$) one gets the desired identity by the following reasoning. W.l.o.g. we may write $u = X \cup \{x_0\}$, $v = X \cup \{x_1\}$, $w = X \cup \{x_2\}$ for an $(n-3)$-element set $X \coloneqq u \cap v \cap w$ and elements $x_i \in \mathcal{A}$ ($i = 0, 1, 2$) such that $\{x_0, x_1, x_2\} \cup X = u \cup v \cup w$. Furthermore, we may assume that $X_0 < x_0 < X_1 < x_1 < X_2 < x_2 < X_3$, where X_0, X_1, X_2, X_3 partitions X (otherwise interchange the labeling of u, v and w; some sets X_i may

of course be empty for $i = 0, \ldots, 3$). Then compute

$$\begin{aligned}
\overline{\lambda}(u,v)\overline{\lambda}(v,w)\overline{\lambda}(w,u) &= \left(\frac{\operatorname{sgn}(X_0, x_0, X_1, X_2, X_3, x_1)}{\operatorname{sgn}(X_0, X_1, x_1, X_2, X_3, x_0)}\right)^{t+1} && (4)\\
&\times \left(\frac{\operatorname{sgn}(X_0, X_1, x_1, X_2, X_3, x_2)}{\operatorname{sgn}(X_0, X_1, X_2, x_2, X_3, x_1)}\right)^{t+1} && (5)\\
&\times \left(\frac{\operatorname{sgn}(X_0, X_1, X_2, x_2, X_3, x_0)}{\operatorname{sgn}(X_0, x_0, X_1, X_2, X_3, x_2)}\right)^{t+1} && (6)\\
&= (-1)^{((|X_2|+|X_3|)+(|X_1|+1+|X_2|+|X_3|))(t+1)} && (7)\\
&\times (-1)^{(|X_3|+(|X_2|+1+|X_3|))(t+1)} && (8)\\
&\times (-1)^{((|X_1|+|X_2|+1+|X_3|)+|X_3|)(t+1)} && (9)\\
&= (-1)^{t+1} && (10)
\end{aligned}$$

to end the proof.

This lemma enables us to make the following definition.

Let $\mathcal{A} \subseteq \mathbb{F}_q^n$ be a representation of an arc. We say that its tangent polynomials are defined canonically with respect to the linear order $\leq$ on $\mathcal{A}$ if they satisfy for all x_0, x_1, X the identity

$$\frac{T_{X\cup\{x_1\}}(x_0)}{T_{X\cup\{x_0\}}(x_1)} = \left(\frac{\operatorname{sgn}(X \cup \{x_1\}, x_0)}{\operatorname{sgn}(X \cup \{x_0\}, x_1)}\right)^{t+1}$$

where $X \subseteq \mathcal{A}$ has $n-3$ elements and $x_0, x_1 \in \mathcal{A} \setminus X$ are distinct.

This simple but effective trick enables us to prove some results of Ball and de Beule avoiding the occurrence of some inconvenient terms in the calculation. Note that in the above definition the tangent polynomials are still only defined up to scalar factor, but their quotients are fixed. In the following we do only work with the tangent polynomials chosen in that manner.

Actually, we shall use new symbols $P(X)$ for the evaluation of tangent polynomials in subsequent calculations.

[abbreviation of tangent polynomial evaluations] Let $\mathcal{A}$ be a representation of an arc in $\mathrm{P}\mathbb{F}_q^n$ such that the tangent polynomials T_Y are defined canonically with respect to some linear order $\leq$ on $\mathcal{A}$. Then we set $P(X) \coloneqq T_{X\setminus\{x\}}(x)$ where x is the biggest element in X.

2 Interpolation formulae

An elementary but particularly nice idea is to use interpolation to capture information about the arc.

There are two basic possibilities to apply interpolation.

[interpolation of the tangent polynomial] Let $\mathcal{A} \subseteq \mathbb{F}_q^n$ be a representation of an arc and $A, B \subseteq \mathcal{A}$ be disjoint subsets with $|A| = t+2$ and $|B| = n-2$. Then

$$\sum_{a\in A} T_B(a) \prod_{z\in A\setminus\{a\}} \det(z, B, a)^{-1} = 0$$

holds or equivalently, when the tangent polynomials are defined canonically with respect to some linear order $\leq$,

$$\sum_{a\in A} P(\{a\}\cup B)\prod_{z\in A\setminus\{a\}}\det(z,\{a\}\cup B)^{-1}=0.$$

As $T_B(x+y)=T_B(x)$ for all $x\in\mathbb{F}_q^n$ and $y\in\langle B\rangle$ we may interpolate the polynomial $\overline{T}_B(x+\langle B\rangle)\coloneqq T_B(x)$ as a homogeneous polynomial of degree t over $\mathbb{F}_q^n/\langle B\rangle$. To do this, pick $a\in A$ to get

$$T_B(x)=\sum_{a'\in A\setminus\{a\}} T_B(a')\prod_{z\in A\setminus\{a,a'\}}\frac{\det(z,B,x)}{\det(z,B,a')},$$

since both sides are polynomials in x of degree t and both are constant on cosets of $\langle B\rangle$ and agree on $t+1$ points of $\mathbb{F}_q^n/\langle B\rangle$ (namely $a'+\langle B\rangle$ for $a'\in A\setminus\{a\}$), for which the right hand side is a LAGRANGE interpolation formula. Replacing x by a and dividing by $\prod_{z\in A\setminus\{a\}}\det(z,B,a)$ one gets

$$T_B(a)\prod_{z\in A\setminus\{a\}}\det(z,B,a)^{-1}=\det(a',B,a)^{-1}\sum_{a'\in A\setminus\{a\}} T_B(a')\prod_{z\in A\setminus\{a,a'\}}\det(z,B,a')^{-1}$$

which is what we wanted to prove. The second formulation in the lemma follows from the fact that the tangent polynomials are defined canonically with respect to an underlying linear order and the definition of $P(X)$ together with mds-segre-simplified.

Another idea is to interpolate the determinants themselves. [interpolation of determinants] Let $A,B,C\subseteq\mathbb{F}_q^n$ such that $\langle A\cup C\rangle=\mathbb{F}_q^n$, $|A|+|C|=n+1$ and $|B|+|C|=n-1$, and let $\leq$ be some linear order on $A\cup B\cup C$. Then we have

$$\sum_{a\in A}\operatorname{sgn}(a,A\setminus\{a\}\cup C)\det(a,B\cup C)\det(A\setminus\{a\}\cup C)=0.$$

Here, sgn is taken with respect to $\leq$.

Picking $a\in A$ and interpolating $\det(\bullet,B\cup C)$ as a linear form in $\mathbb{F}_q^n/\langle C\rangle$ gives

$$\det(x,B\cup C)=\sum_{a'\in A\setminus\{a\}}\det(a',B\cup C)\frac{\det(x,A\setminus\{a,a'\}\cup C)}{\det(a',A\setminus\{a,a'\}\cup C)}$$

which holds as it holds for $x\in A\setminus\{a\}\cup C$ which is a basis of $\mathbb{F}_q^n$. Replacing x by a and rearranging the terms yields

$$\begin{aligned}\det(a,B\cup C)\det(A\setminus\{a\}\cup C)&=\sum_{a'\in A\setminus\{a\}}\det(a',B\cup C)\frac{\det(a,A\setminus\{a,a'\}\cup C)}{\operatorname{sgn}(a',A\setminus\{a,a'\}\cup C)} &(11)\\ &=\sum_{a'\in A\setminus\{a\}}\det(a',B\cup C)\det(A\setminus\{a'\}\cup C)\frac{\operatorname{sgn}(a,A\setminus\{a,a'\}\cup C)}{\operatorname{sgn}(a',A\setminus\{a,a'\}\cup C)} &(12)\\ &=-\sum_{a'\in A\setminus\{a\}}\det(a',B\cup C)\det(A\setminus\{a'\}\cup C)\frac{\operatorname{sgn}(a',A\setminus\{a'\}\cup C)}{\operatorname{sgn}(a,A\setminus\{a\}\cup C)}, &(13)\end{aligned}$$

which is the desired result.

2.1 Manipulation of interpolation identities

For the rest of this section we fix $\mathcal{A} \subseteq \mathbb{F}_q^n$ as a representation of an arc in $\mathrm{P}\mathbb{F}_q^n$ with a linear order $\leq$ explained on it, $P(X)$ as the evaluations of tangent polynomials of $\mathcal{A}$ as defined in tang-pol-eval, $p = \operatorname{char} \mathbb{F}_q$ as the characteristic of the finite field $\mathbb{F}_q$ and $t \coloneqq q + n - 1 - |\mathcal{A}|$ as the degree of the tangent polynomials of $\mathcal{A}$.

Now, the idea is to play with the interpolation identities to reach a contradiction in the case where $t \leq n - 3$ (i.e. $|\mathcal{A}| \geq q + 2$).

First attempt. The proof of the main conjecture for MDS codes of Ball and de Beule for the case in which $n \leq p$ and the classification of $(q+1)$-arcs in that case is based on the following key result which can be derived by elementary means from the interpolation of tangent polynomials.

[Ball & de Beule's ABC lemma] Let $0 \leq r \leq \min\{n, p\} - 1$ and $A, B, C \subseteq \mathcal{A}$ disjoint sets such that $|A| + |B| = r + t + 1$, $|C| = n - 1 - r$. We then have

$$(-1)^r \sum_{\substack{A' \subseteq A \\ |A'| = r}} P(A' \cup C) \prod_{z \in (A \setminus A') \cup B} \det(z, A' \cup C)^{-1} \tag{14}$$

$$= \sum_{\substack{B' \subseteq B \\ |B'| = r}} P(B' \cup C) \prod_{z \in (B \setminus B') \cup A} \det(z, B' \cup C)^{-1}. \tag{15}$$

The proof happens by induction on r. For $r = 0$ the statement is a trivial. Now, suppose the lemma is proven for $r - 1 \geq 0$ and let $r \leq \min\{n, p\} - 1$. Moreover, let $A, B, C \subseteq \mathcal{A}$ be disjoint sets such that $|A| + |B| = r + t + 1$, $|C| = n - 1 - r$. Then pick $a \in A$ and apply the lemma for $r - 1$ and sets $A \setminus \{a\}$, B, $\{a\} \cup C$ (if A and B are empty the lemma is obvious — moreover, the roles of A and B are symmetric). This yields

$$(-1)^{r-1} \sum_{\substack{A' \subseteq A \setminus \{a\} \\ |A'| = r-1}} P(A' \cup \{a\} \cup C) \prod_{z \in (A \setminus A') \cup B} \det(z, A' \cup \{a\} \cup C)^{-1} \tag{16}$$

$$= \sum_{\substack{B' \subseteq B \\ |B'| = r-1}} P(B' \cup \{a\} \cup C) \prod_{z \in (B \setminus B') \cup A \setminus \{a\}} \det(z, B' \cup \{a\} \cup C)^{-1}. \tag{17}$$

Summing over $a \in A$ gives

$$(-1)^{r-1} r \sum_{\substack{A' \subseteq A \\ |A'|=r}} P(A' \cup C) \prod_{z \in (A \setminus A') \cup B} \det(z, A' \cup C)^{-1} \tag{18}$$

$$= \sum_{\substack{B' \subseteq B \\ |B'|=r-1}} \sum_{a \in A} P(B' \cup \{a\} \cup C) \prod_{z \in (B \setminus B') \cup A \setminus \{a\}} \det(z, B' \cup \{a\} \cup C)^{-1} \tag{19}$$

$$= \sum_{\substack{B' \subseteq B \\ |B'|=r-1}} \sum_{a \in A} P(B' \cup \{a\} \cup C) \prod_{z \in (B \setminus B' \cup A) \setminus \{a\}} \det(z, B' \cup \{a\} \cup C)^{-1} \tag{20}$$

$$= - \sum_{\substack{B' \subseteq B \\ |B'|=r-1}} \sum_{b \in B \setminus B'} P(B' \cup \{b\} \cup C) \prod_{z \in (B \setminus B' \cup A) \setminus \{b\}} \det(z, B' \cup \{b\} \cup C)^{-1} \tag{21}$$

$$= -r \sum_{\substack{B' \subseteq B \\ |B'|=r}} P(B' \cup C) \prod_{z \in (B \setminus B') \cup A} \det(z, B' \cup C)^{-1}. \tag{22}$$

Here we used the interpolation of tangent polynomials in the fourth line for the sets $B' \cup C$ and $B \setminus B' \cup A$ when $r-1 \leq |B|$. In the case $|B| < r-1$ the left hand side is zero (as it had been zero before). If $r \leq p-1$ it is a unit and we can divide the above by $-r$ to complete the induction.

We thus immediately obtain

[the case $n \leq p$] If $n \leq p$ then $|\mathcal{A}| \leq q+1$.

Assume that $n \leq p$ and $|\mathcal{A}| \geq q+2$ or equivalently $t = q+n-1-|\mathcal{A}| \leq n-3$. Then apply mds-abc-lemma with $r = |A| = n-1 \leq p-1$ and appropriate subsets B, C (as $\min\{n, |\mathcal{A}| - n\} \leq |\mathcal{A}|/2$, using the dual arc *see* def-dual-arcf necessary we may assume w.l.o.g. that $n+t \leq 2n-3 \leq |\mathcal{A}|$). We have $|B| = t+1 \leq n-2$ and thus the lemma gives

$$(-1)^{n-1} P(A) \prod_{z \in B} \det(z, A)^{-1} = 0$$

which is a contradiction.

This is as we will see the optimal result using *only* the interpolation of the tangent polynomial in the sense that the corresponding system of equations for $t = n-3$ is regular if and only if $n \leq p$ *see* sec-mds-knes

Moreover, in that case the $(q+1)$-arcs can be identified as normal rational curves.

[classification of $(q+1)$-arcs for $n \leq p$] Let $n \leq p$. Then $\mathcal{A}$ is a normal rational curve.

In the case $|\mathcal{A}| = q+1$ one has $t = n-2$. Again, we apply mds-abc-lemma for $r = n-1 \leq p-1$ and $A \subseteq \mathcal{A}$ with $|A| = n$ and appropriate sets $B, C \subseteq \mathcal{A}$ (here $|B| = t = n-2 < r$ and $C = \emptyset$). This gives

$$(-1)^{n-1} \sum_{\substack{A' \subseteq A \\ |A'|=n-1}} P(A') \prod_{z \in (A \setminus A') \cup B} \det(z, A')^{-1} = 0.$$

Applying the above for A and $B_b \coloneqq B \setminus \{b\} \cup \{x\}$ for some fixed point $x \in \mathcal{A} \setminus A$ we obtain the

$n-2$ equations

$$\sum_{a\in A} P(A\setminus\{a\})\prod_{z\in B}\det(z,A\setminus\{a\})^{-1}\frac{\det(b,A\setminus\{a\})}{\det(a,A\setminus\{a\})}\det(x,A\setminus\{a\})^{-1}=0\quad(b\in B).$$

We could also have written $a^*(b)$ (where a^* means an element of the dual basis of A) for the fraction of determinants showing that the matrix $M\in\mathbb{F}_q^{B\times A}$ defined by

$$M\coloneqq(m_{ba})_{(b,a)\in B\times A},\quad m_{ba}\coloneqq\frac{\det(b,A\setminus\{a\})}{\det(a,A\setminus\{a\})}$$

has full rank as its rows are just the coordinate vectors of each $b\in B$ with respect to the basis A. Thus it follows that the matrix $N\coloneqq MD$, where

$$D\coloneqq\operatorname{diag}\left(P(A\setminus\{a\})\prod_{z\in\{a\}\cup B}\det(z,A\setminus\{a\})^{-1}:a\in A\right),$$

has full rank which is the matrix of the linear system mds-class-n-leq-p-keysys in

$$\left(\frac{\det(a,A\setminus\{a\})}{\det(x,A\setminus\{a\})}\right)_{a\in A}.$$

Hence the kernel of this system has dimension $|A|-|B|=n-(n-2)=2$ showing that the image of x for all $x\in\mathcal{A}\setminus A$ under the map

$$\gamma:({\mathbb{F}_q}^\times)^n\to({\mathbb{F}_q}^\times)^n$$

where $({\mathbb{F}_q}^\times)^n\coloneqq\mathbb{F}_q^n\setminus\bigcup_{a\in A}\langle A\setminus\{a\}\rangle$ and

$$\sum_{a\in A}\lambda_a a\mapsto\sum_{a\in A}\lambda_a^{-1}a$$

must lie on a (projective) line i.e. in a two dimensional subspace of $\mathbb{F}_q^n$. Using an appropriate element of $M\in\mathrm{PGL}(n,\mathbb{F}_q)$ which maps $\langle a\rangle\mapsto\langle a\rangle$ for $a\in A$ and $\langle\hat{x}\rangle\mapsto\left\langle\sum_{a\in A}a\right\rangle$ for some $\hat{x}\in\mathcal{A}\setminus A$ we may assume w.l.o.g. that $\hat{a}\coloneqq\sum_{a\in A}a\in\mathcal{A}$. Set $\hat{A}\coloneqq A\cup\{\hat{a}\}$.

Rescaling $\gamma(x)$ ($x\in\mathcal{A}\setminus\hat{A}$) appropriately we obtain scalars α_x such that

$$\alpha_x\gamma(x)=\breve{a}-\hat{a}\lambda_x$$

lie on an affine line parallel to $\langle\hat{a}\rangle$ in $\mathbb{F}_q^n$ (for some $\breve{a}\in\mathbb{F}_q^n$ and $\lambda_x\in\mathbb{F}_q$). This is possible since the point $\langle\hat{a}\rangle$ lies on the same projective line as all $\langle x\rangle\in\mathcal{A}\setminus\hat{A}$ so the latter lie in an affine line parallel to $\langle\hat{a}\rangle$. Changing the parameters if necessary by a translation $x\mapsto x+\mu$ ($\mu\in\mathbb{F}_q$), we may assume that $0=\lambda_x$ for some $x\in\mathcal{A}\setminus\hat{A}$ whence $\breve{a}\in({\mathbb{F}_q}^\times)^n$.

The line $\lambda\mapsto\breve{a}-\hat{a}\lambda$ intersects the n hyperplanes $\langle A\setminus\{a\}\rangle$ (for $a\in A$) in n distinct points (i.e. in the coordinate representation $\breve{a}=\sum_{a\in A}\nu_a a$ all ν_a are distinct for $a\in A$). This holds as

the assumption $\nu_{a'} = \nu_{a''}$ for $a', a'' \in A$, $a' \neq a''$ leads to the contradiction $\{\hat{a}, \check{a}\} \cup A \setminus \{a', a''\} \subseteq \mathcal{A}$ forming a linearly dependent n-set.

Therefore, we may deduce that

$$\{\nu_a : a \in A\} \cup \left\{\lambda_x : x \in \mathcal{A} \setminus \hat{A}\right\} = \mathbb{F}_q$$

is a disjoint union as all $\check{a} - \hat{a}\lambda_x$ have no coordinates equal to zero in the basis A. However, considering the set $\hat{\mathcal{A}} \coloneqq \hat{A} \cup \left\{\gamma^{-1} \circ \alpha_x \circ \gamma(x) : x \in \mathcal{A} \setminus \hat{A}\right\}$ we have a representation of the same arc which is a Cauchy-representation shown in cauchy-rep. So the arc represented by $\mathcal{A}$ is a normal rational curve.

The argument can also be used to prove that the cardinality of an arc in $\mathrm{P}\mathbb{F}_q^n$ $(n \leq p)$ can at most become $q + 1$ (similarly to mds-bound-n-leq-p).

Second attempt. In this paragraph we prove the same result for $n \leq 2p - 2$ and will bring in the interpolation of determinants. A classification of $(q + 1)$-arcs is not given.

[Ball's & de Beule's $ABCDE$ lemma] Let $n > p$ and $0 < r \leq p - 1$ and $0 \leq m \leq \min\{n - 1 - r, t + 2\}$. Moreover, let A, B, C, D and E be disjoint subsets of $\mathcal{A}$ with $|A| = |B| = m$, $|C| = t + 2 - m$, $|D| = n - 1 - r - m$, $|E| = r - 1$ and let there be given bijections $m \to A$ and $m \to B$ such that A_τ, B_τ denote the images of $\tau \subseteq m = \{0, \ldots, m - 1\}$. Then we have

$$0 = \sum_{\substack{C' \subseteq C \\ |C'| = r}} \sum_{\tau \subseteq m} (-1)^{|\tau|} P(A_\tau \cup B_{m \setminus \tau} \cup C' \cup D) \tag{23}$$

$$\times \prod_{\substack{z \in A_{m \setminus \tau} \cup B_\tau \\ \cup (C \setminus C') \cup E}} \det(z, A_\tau \cup B_{m \setminus \tau} \cup C' \cup D)^{-1}. \tag{24}$$

The proof happens by induction on m. We have $n > p$ so we may apply the mds-abc-lemma for $r \leq p - 1$ and sets A, B, C with $|A| = t + 2$, $|B| = r - 1$ and $|C| = n - 1 - r > 0$. This gives

$$0 = \sum_{\substack{A' \subseteq A \\ |A'| = r}} P(A' \cup C) \prod_{z \in (A \setminus A') \cup B} \det(z, A' \cup C)^{-1}.$$

proving the lemma for $m = 0$ when replacing A by C, B by E and C by D.

For the induction step, assume the lemma holds for $m - 1$ and for given A, B, C, D and E with $|A| = |B| = m$, $|C| = t + 2 - m$, $|D| = n - 1 - r - m$, $|E| = r - 1$ pick $a \coloneqq a_m \in A$ and $b \coloneqq b_m \in B$ and apply the induction hypothesis for $\overline{A} \coloneqq A \setminus \{a\}$, $\overline{B} \coloneqq B \setminus \{b\}$, $C \cup \{a\}$, $D \cup \{b\}$, E and $\overline{A}$, $\overline{B}$, $C \cup \{b\}$, $D \cup \{a\}$, E (and $m - 1$), respectively. This yields (the terms where $a \in C'$

on the left hand side and $b \in C'$ on the right hand side cancel out)

$$\sum_{\substack{C' \subseteq C \\ |C'|=r}} \sum_{\tau \subseteq m-1} (-1)^{|\tau|} P(\overline{A}_\tau \cup \overline{B}_{(m-1)\setminus\tau} \cup \{b\} \cup C' \cup D) \tag{25}$$

$$\times \prod_{\substack{z \in \overline{A}_{(m-1)\setminus\tau} \cup \{a\} \cup \overline{B}_\tau \\ \cup (C \setminus C') \cup E}} \det(z, \overline{A}_\tau \cup \overline{B}_{(m-1)\setminus\tau} \cup \{b\} \cup C' \cup D)^{-1} \tag{26}$$

$$= \sum_{\substack{C' \subseteq C \\ |C'|=r}} \sum_{\tau \subseteq m-1} (-1)^{|\tau|} P(\overline{A}_\tau \cup \{a\} \cup \overline{B}_{(m-1)\setminus\tau} \cup C' \cup D) \tag{27}$$

$$\times \prod_{\substack{z \in \overline{A}_{(m-1)\setminus\tau} \cup \overline{B}_\tau \cup \{b\} \\ \cup (C \setminus C') \cup D}} \det(z, \overline{A}_\tau \cup \{a\} \cup \overline{B}_{(m-1)\setminus\tau} \cup C' \cup D)^{-1}. \tag{28}$$

Rearranging this to one side proves the induction.

Applying the above corollary to the condition $|\mathcal{A}| = q + 2$, i.e. $t = n - 3$ leads to

When $|\mathcal{A}| = q + 2$ and $m = n - 1 - r \geq n - p$ we have

$$0 = \sum_{\tau \subseteq m} (-1)^{|\tau|} P(A_\tau \cup B_{m\setminus\tau} \cup C) \prod_{z \in A_{m\setminus\tau} \cup B_\tau \cup E} \det(z, A_\tau \cup B_{m\setminus\tau} \cup C)^{-1}.$$

Since $|C \setminus C'| = t + 2 - m - r = (n-1) - (n-1-r) - r = 0$ the corresponding factors vanish in the product of the last corollary. For the same reason $D = \emptyset$.

[the case $n \leq 2p - 2$] Any arc $\mathcal{A}$ in $\mathrm{P}\mathbb{F}_q^n$ with $n \leq 2p - 2$ satisfies the bound $|\mathcal{A}| \leq q + 1$.

We may assume that $n > p$ by the previous work. Apply the previous corollary for $r = p - 1$, then $|E| = p - 2$, $|C| = p - 1$ and $|A| = |B| = n - p$. Write E as $E = F \cup G$ where $|F| = 2p - 2 - n$ (here we use the assumption) and $|G| = n - p > 0$. Rewriting the equation of in the last corollary delivers

$$0 = \sum_{\tau \subseteq m} (-1)^{|\tau|} P(A_\tau \cup B_{m\setminus\tau} \cup C) \prod_{z \in A_{m\setminus\tau} \cup B_\tau \cup F \cup G} \det(z, A_\tau \cup B_{m\setminus\tau} \cup C)^{-1}.$$

We now aim to prove the following equation for $0 \leq s \leq n - p$ for which the above is the base of induction (inducting on $s \coloneqq |D| = |F| - (2p - 2 - n)$)

$$0 = \sum_{\tau \subseteq m} (-1)^{|\tau|} P(A_\tau \cup B_{m\setminus\tau} \cup C) \prod_{w \in D} \det(w, A_\tau \cup B_{m\setminus\tau} \cup C) \prod_{z \in A_{m\setminus\tau} \cup B_\tau \cup F \cup G} \det(z, A_\tau \cup B_{m\setminus\tau} \cup C)^{-1}.$$

for $D \subseteq A$ an s-element set (which is possible since $|A| = n - p \geq s$).

For the induction step we pick $d \in D$ and $g \in G$, $f \in F$, assume the hypothesis to be proven for $s - 1$ and apply this to our sets A, B, C, $D \setminus \{d\}$, $F \setminus \{f\}$, $G \setminus \{g\} \cup \{f\}$

$$0 = \sum_{\tau \subseteq m} (-1)^{|\tau|} P(A_\tau \cup B_{m\setminus\tau} \cup C) \prod_{w \in D\setminus\{d\}} \det(w, A_\tau \cup B_{m\setminus\tau} \cup C) \quad \times \det(g, A_\tau \cup B_{m\setminus\tau} \cup C) \prod_{z \in A_{m\setminus\tau} \cup B_\tau \cup F \cup G} \det(z$$

Now, we use in the interpolation formula for the determinants as given in mds-tan-poly-interpol-det. Multiplying the above by

$$\operatorname{sgn}(g, \{d\} \cup (G \cup \{f\}) \setminus \{g\} \cup C) \det(\{d\} \cup (G \cup \{f\}) \setminus \{g\} \cup C)$$

and summing over $g \in G \cup \{f\}$ gives (by interpolation of determinants)

$$0 = -\operatorname{sgn}(d, G \cup \{f\} \cup C) \det(G \cup \{f\} \cup C) \sum_{\tau \subseteq m} (-1)^{|\tau|} P(A_\tau \cup B_{m\setminus\tau} \cup C) \prod_{w \in D\setminus\{d\}} \det(w, A_\tau \cup B_{m\setminus\tau} \cup C)$$

where we can omit the sgn and det at the beginning to see that we are done with the induction step. Of course, the above argument does only work for $s = |D| \leq |A| = n - p$. Applying the formula which we have just proven for $s = n - p$ (i.e. $D = A$) we get

$$P(B \cup C) \prod_{w \in A} \det(w, B \cup C) \prod_{z \in A \cup F \cup G} \det(z, B \cup C)^{-1} = 0$$

since all terms where $\tau \neq \emptyset$ vanish. This clearly is a contradiction. Lastly, we have to verify that $A \cup B \cup C \cup F \cup G$ is not bigger than $q + 2$. Adding the cardinalities leads to

$$|A \cup B \cup C \cup F \cup G| = 2(n - p) + (p - 1) + (p - 2) + (n - p) = 3n - 3 - p.$$

But this is no restriction since $p \leq \sqrt{q}$ and thus $n \leq 2\sqrt{q}-2$ so $3n-3-p < 3n-3 \leq 6\sqrt{q}-9 \leq q$.

The author's proposal is to call the above the A–G lemma.